HIPAA: Practical Application from a Non-Lawyer's Perspective

Jim Kelly
HIPAA Privacy Officer (Ret.)
Chesterfield Fire & EMS

Disclaimer: I am not a lawyer!

Although I assume everyone will think the information in this presentation is intended to make you want to hire me immediately, I see that law firms have these fancy disclaimers and I sure like tugging on their capes…. So here goes:

1. The information in this presentation is not intended to create an attorney-client relationship. Frankly, you don't want it to do so either. First, I'm not a lawyer. And since the presentation can in theory be attended by any EMS provider on the planet, claiming that you have an attorney-client relationship as a result of this presentation, even if I was a lawyer, would lead to an immediate claim that you've waived the privilege. If you're crazy enough to want that outcome, I wouldn't want to be your lawyer anyway. Even if you contact me after the class, that would not give rise to an attorney-client relationship either, even if I was a lawyer. Did I mention that I'm not a lawyer? Don't you feel better now?

2. Don't send me any confidential information unless I expressly agree that I have an attorney-client relationship with you—which I can't because I'm not a lawyer. After all, I might have a conflict of interest (that is pretty unlikely, but you never know for sure), especially if I was a lawyer. So be smart and safe and keep it confidential until I say it's okay to send stuff to me … or until a lawyer says it's OK to send it to him/her. Or me.

3. Any references like web sites that I might mention are not under my control. Those sites are responsible for the content of those sites. The sun, the moon and the rotation of the Earth are not under my control either. I'm working on it, but don't hold your breath, and don't try to make me responsible for other sites, bad weather, global warming or any malady that befalls you. If you try, I may have to send my crack in-house security team to visit you.

4. The world is an ever-changing place, which means that content can become outdated quickly. While I've taken great pains to try to bring you the most current information, I can't guarantee that everything is timely, so don't rely on the timeliness or accuracy of the information presented here. Only a lawyer would put out information to impress you and then say "don't rely on it." Did I mention that I'm not a lawyer? Oh, never mind—still don't rely on it absolutely. Take it upon yourself and research it thoroughly. Even lawyers don't know it all!

In other words, if you violate HIPAA, it's not my fault!

Objectives

- Review of HIPAA basics
- Penalties for violations
- What HIPAA protects and how
- Major operational issues and questions
- HIPAA breaches
- What's in the pipeline

Review of Basics

- What is HIPAA anyway?
- Who does HIPAA apply to?
- If I'm not a HIPAA covered entity, do I have to worry about patient privacy?
- What are HIPAA's major rules that affect me?

Possible Fines

- For unknowingly violating: $100 - $50K per violation
- For knowingly violating: $1000 - $50K per violation
- For violation from willful neglect
  - Corrected: $10K - $50K per violation
  - Uncorrected: $50K per violation
  - Mandatory
- $1.5M annual maximum

Criminal Prosecution and Prison

- Access, use, or disclosure of PHI with malicious intent or for personal gain
  - Theft
  - Fraud
  - Extortion
  - Sale
  - Snooping

Privacy Rule vs. Security Rule

- What does the Privacy Rule protect and how does it protect it?
- What does the Security Rule protect and how does it protect it?

At the Core of HIPAA Protection: Protected Health Information (PHI)

- Individually identifiable health information
- Past, present or future health care or payment

PHI

- Where does PHI exist and where does it come from?
- In what form can we find PHI?
- What may we do with PHI?
  - TPO uses and disclosures
- Do we need the patient's permission to use or disclose PHI?
- What is the "Minimum Necessary" standard?

Operational Issues

Before the Call

- Who must be trained?
- May we have ride-alongs?

Dispatch and Response

- May the dispatch center transmit PHI over the radio?
- May we share PHI over the radio with other responding agencies?

On Scene

- May we discuss the patient's condition with first responders or other on-scene providers?
- May we discuss PHI with the patient's family members?
- How about with parents of minors?

On Scene

- A police officer asks if our patient has been drinking. May we tell him?
- When may we provide information to law enforcement?
- May we give a TV or newspaper reporter details about the call?
- May I take a picture of an accident scene with my cell phone camera?

Enroute to and at the Hospital

- May we transmit PHI to the receiving facility?
- May we give a verbal report to the ER staff?
- May we give the hospital a PCR copy?
- May we obtain a face sheet or billing information from the facility?

Any Time During the Call

- What is this Notice of Privacy Practices thing and what do I do with it?
- The patient asks you to bill him directly and not send the bill to the insurance company. What do you do?

After the Call

- May we get follow-up information on our patient from the hospital?
- We suspect our patient is a victim of abuse. May we notify CPS or APS?
- May we critique the call with the Chief or the QA Coordinator?

After the Call

- May we describe our patient encounter in a training class?
- May we discuss the call with a counselor during CISD?

After the Call

- May we report a member's line-of-duty injury to the Chief?
- May we provide details of the injury to other members?
- The supervisor or department safety officer investigates the injury. May s/he provide details of the injury to the Chief?

After the Call

- We transported a member from his home for chest pain. May we report that to the Chief?
- May we give a copy of the PCR to the Chief because the patient is a friend of his?
- We transported a patient from a house fire. May we give PHI to the fire investigator?

Are These HIPAA Violations?

- A bystander overhears your patient interview
- A colleague happens to glance your way as you enter your PCR on the computer
- A citizen hears your HEAR report on his scanner

Are These HIPAA Violations?

- You give someone else your password
- You fax a PCR to the wrong number
- You throw your “field sheet” in the trash after the call
- You leave the PCR open on the computer while you run another call
- You leave your Toughbook on the scene
- You copy patient data onto your flash drive to do QA work at home

What is a Breach?

"The acquisition, access, use, or disclosure of ***unsecured*** PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI."

What is “Unsecured” PHI?

“PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in HHS [U.S. Department of Health and Human Services] guidance.”

Breaches

- What are some examples of breaches?
- What do I if I discover a breach?
- What will happen to me if I report a breach?
- What should the agency do if I report a breach?

UCLA medical officials say patient information data stolen

November 4, 2011 | 4:13 pm

The UCLA Health System is warning thousands of patients that their personal information was stolen and they are at risk of possible identity theft, officials said in a statement released Friday.

Officials don't believe the information has been accessed or misused but are referring patients to a data security company if their name and credit are affected.

Altogether, 16,288 patients' information was taken from the home of a physician whose house was burglarized on Sept. 6, according to the UCLA Health System.

The physician works for UCLA Faculty Practice Group, whose doctors see patients at the outpatient clinics and the four inpatient hospitals: Ronald Reagan UCLA Medical Center, Santa Monica UCLA Medical Center and Orthopedic Hospital, Mattel Children's Hospital and Resnick Neuropsychiatric Hospital.

The stolen patient information included first and last names as well as some birth dates, medical record numbers, addresses and medical information, officials said. It did not include Social Security numbers, credit card or insurance details. The patient information was from 2007 through 2011.

The data were on the physician's external hard drive, officials said. Though the hard drive was encrypted, a piece of paper with the password was nearby and is also missing. The physician notified UCLA the next day and officials began identifying patients affected.

The theft is not the first breach at UCLA. Between 2005 and 2009, hospital officials were repeatedly caught and fired for reviewing, without authorization, the medical records of dozens of celebrities, including Britney Spears and Farrah Fawcett. That prompted a state law imposing escalating fines on hospitals for patient privacy lapses. State regulators later fined Ronald Reagan UCLA Medical Center in connection with privacy breaches involving the records of Michael Jackson.

What's in the Pipeline

- New proposed accounting rules for disclosures to external entities:
  - For TPO purposes
  - That are not permitted under HIPAA, unless the patient has already received breach notification
  - For public health activities
  - For judicial and administrative proceedings
  - For law enforcement purposes
  - To avert a serious threat to health and safety
  - For military and veterans' activities
  - For workers' compensation

What's in the Pipeline

- New proposed patient right: access report for e-PHI
  - Date of access
  - Time of access
  - First and last name of person who accessed if available
  - What information was accessed
  - The action of the person who accessed (create, modify, delete, print, etc.)
- Systematic compliance audits

Get in front of the proposed changes now!

Thank you!

Jim Kelly
emtp@jbkelly.us